**ÁREA TECNOLOGÍAS DE INFORMACIÓN**
OFICINA DE GERENCIA Y PRESUPUESTO

**POLÍTICA NÚM. ATI-003**

**FECHA DE EFECTIVIDAD:** 15 de diciembre de 2004
**FECHA DE REVISIÓN:** 7 de noviembre de 2016

**TEMA:** SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

## DESCRIPCIÓN

Esta Política consiste de directrices generales que permitirán a las agencias establecer controles adecuados en sus sistemas electrónicos de información para garantizar la confidencialidad, la integridad y la disponibilidad de la información que manejan.

La misma deroga y sustituye la Política Núm. TIG-003, conocida como Seguridad de los Sistemas de Información, revisada el 12 de septiembre de 2007.

## BASE LEGAL

Esta Política se emite al amparo de la Ley Núm. 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico". De conformidad con el Artículo 4 de la Ley 151, la OGP es la responsable de administrar los sistemas de información e implementar las normas y procedimientos relativos al uso de las tecnologías de la información a nivel gubernamental. A tales fines, tendrá la facultad para instrumentar desarrollar un andamiaje que garantice controles efectivos con relación a la seguridad de los sistemas de información que sustentan las operaciones y activos gubernamentales. *Id.,* Art. 5, inciso (i). Corresponde a las agencias cumplir con lo dispuesto en la Ley 151, las políticas de manejo de información y los estándares tecnológicos relativos a la Informática emitidos por la OGP, y comunicar las mismas de manera rápida y efectiva a su personal. *Id.,* Art.7, incisos (g) y (h).

## ALCANCE

Esta Política aplica a todas las agencias de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, que en virtud de la Ley Núm. 151-2004, según enmendada, conocida como la "Ley de Gobierno Electrónico", tienen o planifican tener sistemas computadorizados de información, independientemente de su costo y origen de los fondos. Asimismo, aplica a cualquier otro organismo gubernamental que no sea una agencia, en cuanto a aquellos particulares que se disponga.

## ACTUALIZACIÓN DE LA POLÍTICA

El Área de Tecnologías de Información (ATI) de la OGP es responsable de la actualización de la política pública relacionada con las tecnologías de información y comunicación. En virtud de esta facultad, se actualiza la política concerniente a la seguridad de los sistemas de información.

## POLÍTICA

Toda agencia adscrita a la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico deberá seguir las siguientes políticas de seguridad en sus sistemas de información. Los usuarios de los Servicios de la Red Interagencial que no sean agencias (i.e. municipios) están sujetos al cumplimiento de las secciones E, J y K de esta política para poder hacer uso de los Servicios de la Red Interagencial. Es responsabilidad de cada organismo el desarrollo y publicación de políticas y procedimientos aplicables para cumplir la política aquí delineada.

### A. Análisis de Riesgos

1. Cada agencia deberá implantar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada y/o maliciosa. Para ello deberá llevar a cabo análisis de riesgos que incluya:

    a. Inventario de activos de sistemas de información que incluya el equipo, los programas (ver sección de Definiciones) y los datos. Todos los activos deberán ser clasificados de acuerdo al nivel de importancia para la continuidad de las operaciones. En particular, los datos electrónicos deberán ser clasificados de acuerdo a su nivel de confidencialidad. Esto permitirá establecer qué es lo que se va a proteger.

    b. Identificar las posibles amenazas contra los sistemas de información (i.e. robos, desastres naturales, fallas, virus, acceso indebido a los datos, etc.) junto con un análisis del impacto en las operaciones y la probabilidad de que ocurran esas amenazas. Esto permitirá establecer con qué se van a proteger los activos identificados anteriormente.

### B. Continuidad

1. El análisis de riesgo será la base para desarrollar un Plan de Continuidad que incluya un Plan para Recuperación de Desastres y un Plan para la Continuidad de las Operaciones.

2. Establecer procedimientos de resguardo (*backup*) recurrentes de la información, de programas y de sistemas esenciales.

3. Las facilidades de sistemas de información deberán estar colocadas en un área donde sea menor la probabilidad de daños por fuego, inundaciones, explosiones, disturbios civiles y otros desastres.

### C. Políticas de Seguridad Adicionales

1. Las políticas de seguridad de este documento son solo el fundamento para unas políticas más detalladas desarrolladas por cada agencia. Será responsabilidad de cada agencia el desarrollar políticas específicas de seguridad tomando en cuenta las características propias de los ambientes de tecnología de la agencia, particularmente sus sistemas de misión crítica. Las políticas desarrolladas por la OGP para su uso interno podrán ser utilizadas como modelos iniciales en el desarrollo de las políticas específicas de cada agencia.

2. Las políticas aquí establecidas no podrán ser invalidadas por las políticas particulares desarrolladas en cada agencia.

**D. Leyes y Reglamentos**

Las políticas y procedimientos de seguridad deberán estar de acuerdo a la legislación y los reglamentos vigentes que apliquen.

**E. Controles Generales**

1. Las agencias deberán instalar controles automáticos para la prevención y detección de programas no deseados (i.e. virus, spyware, adware y updates automáticos).

2. La seguridad de la información deberá ser parte integral del diseño de cualquier programa de aplicación que se adquiera o desarrolle la agencia para facilitar las operaciones de la agencia y/o mejorar el servicio a los ciudadanos.

3. La información y los programas de aplicación en las operaciones de la agencia deberán tener controles de acceso para su utilización de tal manera que solamente el personal autorizado pueda ver los datos o acceder a las aplicaciones (o la parte de las aplicaciones) que necesita utilizar. Estos controles deberán incluir mecanismos de autenticación y autorización.

4. Todos los mecanismos de autenticación deberán incluir una contraseña combinada de números, letras y caracteres especiales, no menor de ocho (8) caracteres.

5. Cambio de contraseñas

   a. Todas las contraseñas de nivel administrativo se deben cambiar como mínimo cada cuatro (4) meses.

   b. Todas las contraseñas de usuarios se deben cambiar como mínimo cada seis (6) meses.

6. Los privilegios de acceso de los usuarios deberán ser reevaluados regularmente.

7. Deberán existir procesos que permitan monitorear las actividades de los usuarios en aquellos activos sensitivos que lo ameriten.

8. Si se va a disponer de equipo que contiene información sensitiva deberá hacerse de forma segura con un método que no permita acceder los datos una vez el equipo esté fuera de las facilidades de la Agencia.

9. Las agencias deberán establecer los controles necesarios para asegurar aquellos equipos que han estado fuera de la agencia no represente un riesgo a sus sistemas. Ello incluye revisar y requerir auditorías de dichos equipos al ingresarlos a sus sistemas.

10. Las agencias deberán establecer los controles necesarios para evitar que de forma intencionada o accidental se inicien ataques desde sus redes internas hacia otros sistemas de información externos.

11. Cada agencia será responsable de diseñar y mantener la seguridad de sus sistemas de información.

12. Se recomienda a las agencias realizar auditorías de seguridad al menos una vez al año.

**F. Manejo de Incidentes**

1. Las agencias deberán desarrollar procedimientos para detectar, reportar y responder a incidentes de seguridad incluyendo límites para esos incidentes en términos de tiempo máximo y mínimo de respuesta.

2. Todos los empleados y contratistas deberán conocer los procedimientos para informar los diferentes tipos de incidentes.

**G. Manejo de Cambios**

Cada agencia es responsable de diseñar procedimientos que permitan que los cambios a la seguridad de los sistemas sean realizados y documentados adecuadamente y que esta documentación a su vez sea asegurada.

**H. Adiestramientos**

1. Cada agencia es responsable de proveer adiestramientos al personal para que estén al tanto de los controles de seguridad y los beneficios correspondientes.

2. El personal de sistemas de información y telecomunicaciones deberá estar adiestrado y mantenerse actualizado sobre los aspectos de seguridad de sus áreas.

3. Se deben proveer mecanismos para capacitar a todos los empleados periódicamente.

**I. Controles Físicos**

1. El acceso a las facilidades de sistemas de información deberá estar controlado para que solo el personal autorizado pueda utilizarlas.

2. Cualquier equipo usado fuera de la agencia deberá estar autorizado por la gerencia o persona designada, y deberá haber procedimientos para controlar su utilización.

## J. Internet

1. La comunicación con Internet desde adentro de la agencia deberá estar controlada por un *"firewall"*. Las agencias deberán desarrollar las políticas de uso de Internet y de correo electrónico (ver Política Núm. ATI-008, USO DE SISTEMAS DE INFORMACIÓN, DE LA INTERNET Y DEL CORREO ELECTRÓNICO) y utilizar el *firewall* (Servidor de Seguridad de Computadoras y Redes)(ver Política Núm. ATI-014, MANEJO DE LOS *FIREWALLS)* como uno de los mecanismos de control de esas políticas.

2. Las agencias establecerán controles de uso de internet para evitar el uso no adecuado del mismo. Se debe establecer como mínimo una política que bloquee el acceso a páginas pornográficas.

3. Si existe la necesidad de acceder a la red interna desde afuera de las instalaciones de la agencia (por ejemplo, para que un empleado realice un trabajo en un programa de aplicación desde Internet), deberán existir los controles de autenticación, autorización, confidencialidad, integridad y monitoreo necesarios para proteger los sistemas y la información.

4. Si se determina que hay datos sensitivos pasando a través de redes que no son seguras (como Internet o redes inalámbricas), se deberán tener los controles necesarios para garantizar la confidencialidad, como por ejemplo, el uso de cifrado.

5. Toda agencia que desarrolle un programa de aplicación para brindar servicios de la agencia a los ciudadanos a través de Internet deberá asegurarse de que toma en consideración los siguientes elementos en su estudio de viabilidad para la implantación del programa:

   a. Un diseño de seguridad.

   b. La integración de mejores prácticas de seguridad en programación para evitar el acceso no autorizado y/o malicioso a través de Internet.

   c. Un *"firewall"* que permita controlar el acceso al programa desde Internet.

   d. Asegurar que si el servicio que está disponible maneja datos sensitivos, sea instalado en una red alterna. En este caso, el programa deberá funcionar en una red alterna y segura que permita el acceso desde Internet y a la misma vez permita un acceso controlado a la red interna para el intercambio controlado y monitoreado de datos.

   e. Cerciorarse que si el servicio ofrecido a través de Internet maneja datos sensitivos existe implantado un sistema de detección/prevención de intrusos.

## K. Servicios Suministrados por Contratistas

1. Es necesario mantener la seguridad de los sistemas de información aun cuando el manejo y el control de parte o de todos los procesos ha sido delegado a un tercero.

2. Los contratos con terceros deberán incluir la salvaguarda de los activos sensitivos, especialmente cuando los servicios contratados incluyen el manejo de estos activos fuera de las facilidades de la Agencia.

3. Si el servicio suministrado por terceros incluye que parte de los procesos corren en las instalaciones de los contratistas, deberán establecerse controles de mutuo acuerdo para proteger la información y estos acuerdos deberán ser parte del contrato.

4. Todo contrato con terceros deberá incluir la certificación de revisión de seguridad conocida como SOC-2 y la misma debe estar vigente.

**EXENCIONES**

Ninguna

**DEFINICIONES**

**Adware** – Es un programa que se instala inadvertidamente en una computadora y que su principal propósito es desplegar ante el usuario anuncios y propaganda pero también puede tener un comportamiento como el *spyware*.

**Agencia** – Significa cualquier junta, cuerpo, tribunal examinador, comisión, corporación pública, oficina independiente, división, administración, negociado, departamento, autoridad, persona, entidad o cualquier instrumentalidad de la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico, según se dispone en el Artículo 2, inciso (b) de la Ley 151-2004, *supra.*

**Autenticación** – Es el proceso por el cual una persona presenta información que lo identifica ante un sistema de información y el sistema compara la información contra su base de datos para validarla.

**Autorización** – Es el proceso por el cual se adjudican privilegios específicos a una persona para el uso de recursos en los sistemas de información.

**Confidencialidad** – Es la característica que se le da a una información para que pueda ser vista solamente por personas autorizadas.

**Cifrado** – Es el proceso por el cual unos datos se transforman en información no entendible por aquellos que no están autorizados a verlos.

**Datos sensitivos** – Datos que contienen información financiera, de los ciudadanos, de los recursos humanos u otra información crítica para la operación de la agencia.

**Firewall (Servidor de Seguridad de Computadoras y Redes)** – Aplicación, equipo o conjunto de ambos que protege los recursos de la red de accesos no autorizados. En el caso de las aplicaciones son programas que residen en una computadora o en un equipo especializado y que permiten controlar el tráfico de información entre varias redes. Tradicionalmente protegen la red interna de una entidad del acceso indebido de usuarios que vienen de Internet.

**Integridad** – Es el proceso que permite proteger información de alteraciones indebidas.

**Programa** – Conjunto de instrucciones que permite que una computadora lleve a cabo una función. Puede haber **programas de sistema** que controlan el funcionamiento de las computadoras y de las redes de informática y también **programas de aplicación** que facilitan y/o automatizan las operaciones de una entidad para que no tengan que ser llevadas a cabo de forma manual.

**Ransomeware** – Es un programa que se instala inadvertidamente en una computadora y está diseñado para bloquear accesos a los sistemas hasta que se pague una suma de dinero.

**Seguridad de Informática –** Protección de los sistemas de información en contra del acceso o modificación física o electrónica de la información; protección en contra de la negación de servicios a usuarios autorizados o de la disponibilidad de servicios a usuarios no autorizados; las políticas, normas, medidas, proceso y herramientas necesarias para detectar, documentar, prevenir y contrarrestar los ataques a la información o servicios antes descritos; los procesos y herramientas necesarias para la restauración de la información o los sistemas afectados por las brechas en la seguridad; disponibilidad y protección de los recursos requeridos para establecer dicha seguridad.

**Sistema de Detección y Prevención de Intrusos** – Es un programa que reside en una computadora o en un equipo especializado y que permite detectar ataques o intentos indebidos de acceso hacia un sistema de información.

**Spyware**– Es un programa que se instala inadvertidamente en una computadora y que propaga sin autorización información sobre el usuario de la computadora y sus hábitos de utilización de Internet.

**ANEJOS**

Ninguno

**REFERENCIAS**

Ley 151-2004, según enmendada, conocida como "Ley de Gobierno Electrónico".
Política Núm. ATI-008, sobre USO DE SISTEMAS DE INFORMACIÓN, DE LA INTERNET Y DEL CORREO ELECTRÓNICO, revisada el 7 de noviembre e de 2016
Política Núm. ATI-014, MANEJO DE LOS *FIREWALLS,* del 7 de noviembre de 2016

**ANTECEDENTE**

Política Núm. TIG-003, conocida como Seguridad de los Sistemas de Información, revisada el 12 de septiembre de 2007.